II. SPECIFICATION AMENDMENTS

Please replace the paragraph/section beginning on page 1, line 1

~~DEVICES~~ SECURE E-COMMERCE TRANSACTIONS UTILIZING SET SECURITY PROTOCOLS AND EMV CRYPTOGRAMS

Page 10, line 26, to Page 11, line 6

This initiates a request for payment startup message ~~22~~ 29 which is sent from the mobile station to the merchant server 12. This signal can either be of a standard type in which case the merchant server 12 responds with a payment initialisation message 23 which indicates that payment is to be carried out in accordance with the EMV standard or alternatively the mobile phone 10 may already be provided with the information that the merchant server supports only EMV transactions. In this case the startup message ~~22~~ 29 could be adapted to refer specifically to the startup of an EMV transaction.

Page 11, line 7-17

In order to indicate that the merchant server supports EMV transactions the payment initialisation message 23 is a modified SET message. The difference in architecture, ie the ability of the merchant server to accept SET or EMV transactions can be notified in an additional field in the standard SET payment initialisation message. This modified initialisation message 23 can alternatively include an additional or a modification of an existing SET data field from the standard SET payment initialisation message 15 shown in figure 1. For example the standard SET specification specifies a field SET-brand which is transferred from the merchant to client informing the user whether Visa, Master Card or other card be used and giving a URL for a logo. This field can be modified to having the text "EMV" and URL for the merchant address. Or a new field EMV-merchant with URL as value may be added to the message.

Page 12, line 33, to page 13, line 14

In order to do this the EMV card handling process 24 calculates an EMV cryptogram for use in encrypting and decrypting the transferred data. The EMV cryptogram is calculated using data from the modified SET payment initialisation message 23 and information stored in the mobile phone 10 itself. This is similar to that described in relation to Figure 1. Once calculated this EMV cryptogram can be communicated to the merchant server using an open session message 25. Thereafter the merchant server 12 and mobile phone 10 can communicate together via the gateway 11 as is known in the art utilising various signals (not shown). This includes a purchase request signal 26 from the merchant server 12 to a card issuer internet payment gateway (IPGW) 27. This is via standard EMV protocol signals. The gateway forwards the message to the card issuer server. The card issuer can then authorise a transaction depending upon the credit rating or status of the subscriber's account. The result 28 of this authorisation is transmitted to the merchant server via the IPGW 27. The merchant server 12 then notifies the user (would-be purchaser) via a standard acknowledge result message ~~22~~ 30. It will be understood that the IPGW is only one of a number of ways in which merchants and/or banks could be contacted.